**常见工具的使用**

目录

[1． 进程监控 2](#_Toc3902)

[1.1 ProcessMonitor 2](#_Toc1869)

[2． 网络监听 6](#_Toc27880)

[2.1 Fiddler 6](#_Toc12656)

[3． 进程钩子 7](#_Toc10175)

[3.1 Procexp 7](#_Toc19790)

[4． 系统工具 10](#_Toc1697)

[4.1(磁盘硬盘占用率分割工具)SpaceSniffer 10](#_Toc21074)

[5． 其他工具 12](#_Toc26416)

[5.1UltraEdit-32 12](#_Toc25592)

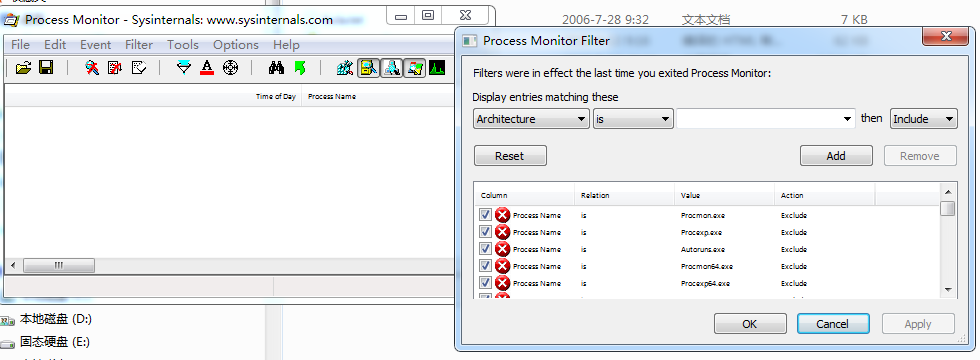
# 进程监控

## 1.1 ProcessMonitor

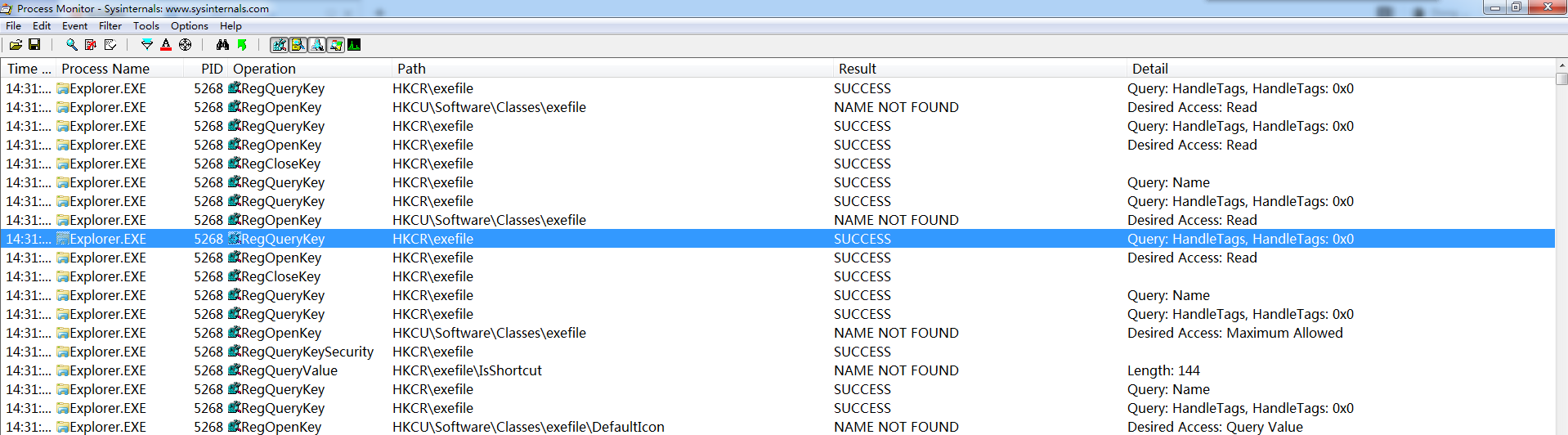
### **ProcessMonitor工具可实时显示文件系统、注册表、进程/线程的活动的等。**

* 操作步骤及演示

步骤一：双击打开process monitor工具。可看到一个弹框是process monitor filter过滤条件框。可事先输入需要过滤的条件或者获取所需要包含的条件。初次使用者可以点击reset按钮，恢复默认配置，之后点击ok进到界面。等获取完日志后再添加过滤条件即可。

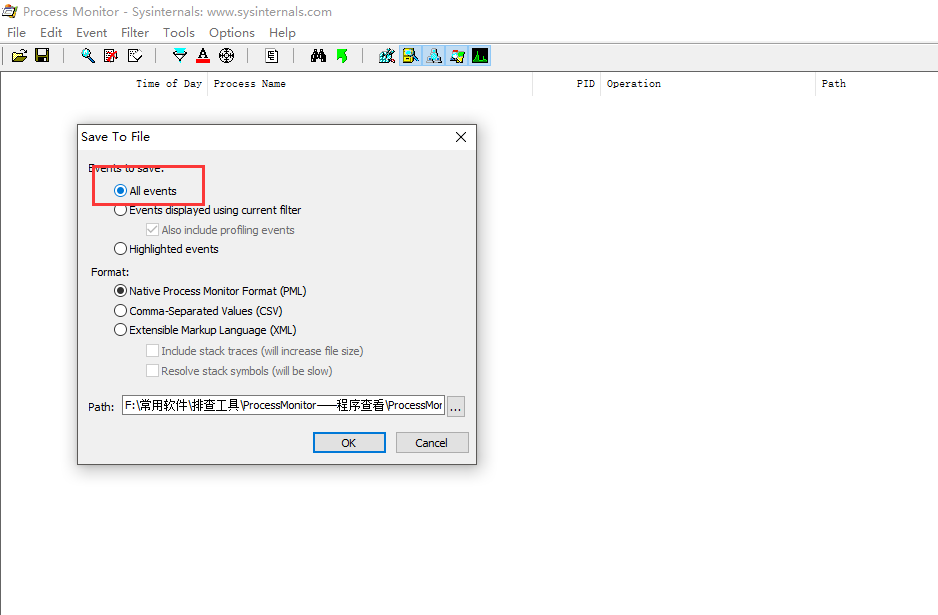


步骤二：打开软件后界面如下图所示



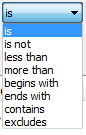
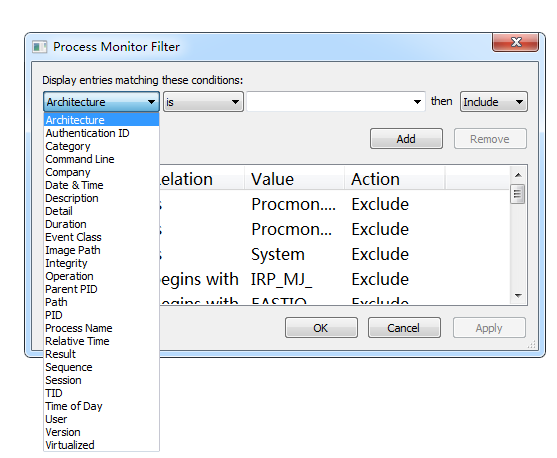
可以看到软件里面看到有一个放大镜按钮：，这个按钮如果是打叉就是关闭停止状态，没有进行获取日志，此时点击一下，就是启动，开始获取日志。橡皮擦按钮的含义是：清除日志。

获取日志的过程：打开软件-点击放大镜按钮停止软件-点击橡皮擦按钮清除无效日志-再次点击放大镜按钮开始获取日志-操作需要采集的过程（比如引起问题的过程，重现问题）-问题出现就可点击放大镜按钮停止获取日志-选择左上角的File-save保存-All events所有事件-path保存路径-ok保存。

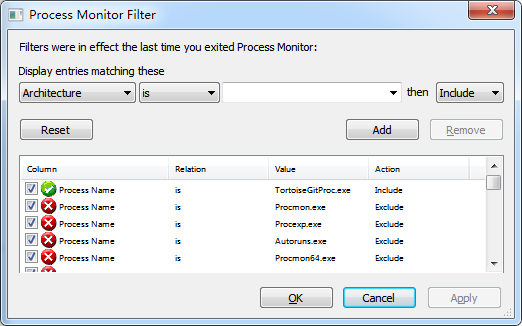


保存日志后可到相关的文件夹将日志Logfile.PML压缩打包发回来给对应的研发人员或者发回来自己进行查看。

1. 查看日志可根据具体需要来设置过滤条件。过滤按钮：可设置过滤条件。如下图所示，包含很多条件。常用条件：Architecture（operation、path、process name ......），（is、is not、less than、more than、begins with、ends with、contains、excludes），常用设置，包含某个进程。可选process name contains XXX.exe或者path contains xxx.pdf等。对应时间，查看对应的进程操作过程，可判断需要的进程或者是需要设置解密的路径等。



步骤三：获取到一份logfile日志后，运行process monitor去打开。点击设置过滤条件。



1. 常规使用字段

path（路径），一般选择contains,然后输入操作文件名称、路径或者文件后缀如.doc等

operation（操作），一般选择contains，然后输入内容可以参考以下列表含义

* CreateFile：创建文件时触发；
* WriteFile：表示写操作，依照文件大小可能产生多条；
* ReadFile：表示读操作，一次读会产生很多条；
* SetAllocationInformationFile：改写文件时触发；
* SetEndOfFileInformationFile：改写文件时触发；
* SetRenameInformationFile：重命名时触发；
* SetDispositionInformationFile：删除文件时触发。
* exit：进程退出的动作。(一般用于ldcore导致软件打开异常，可获取日志查看exit进程添加coreconfig过滤进行测试)

detail（细节），一般选择contains，然后输入create

contains(包含)

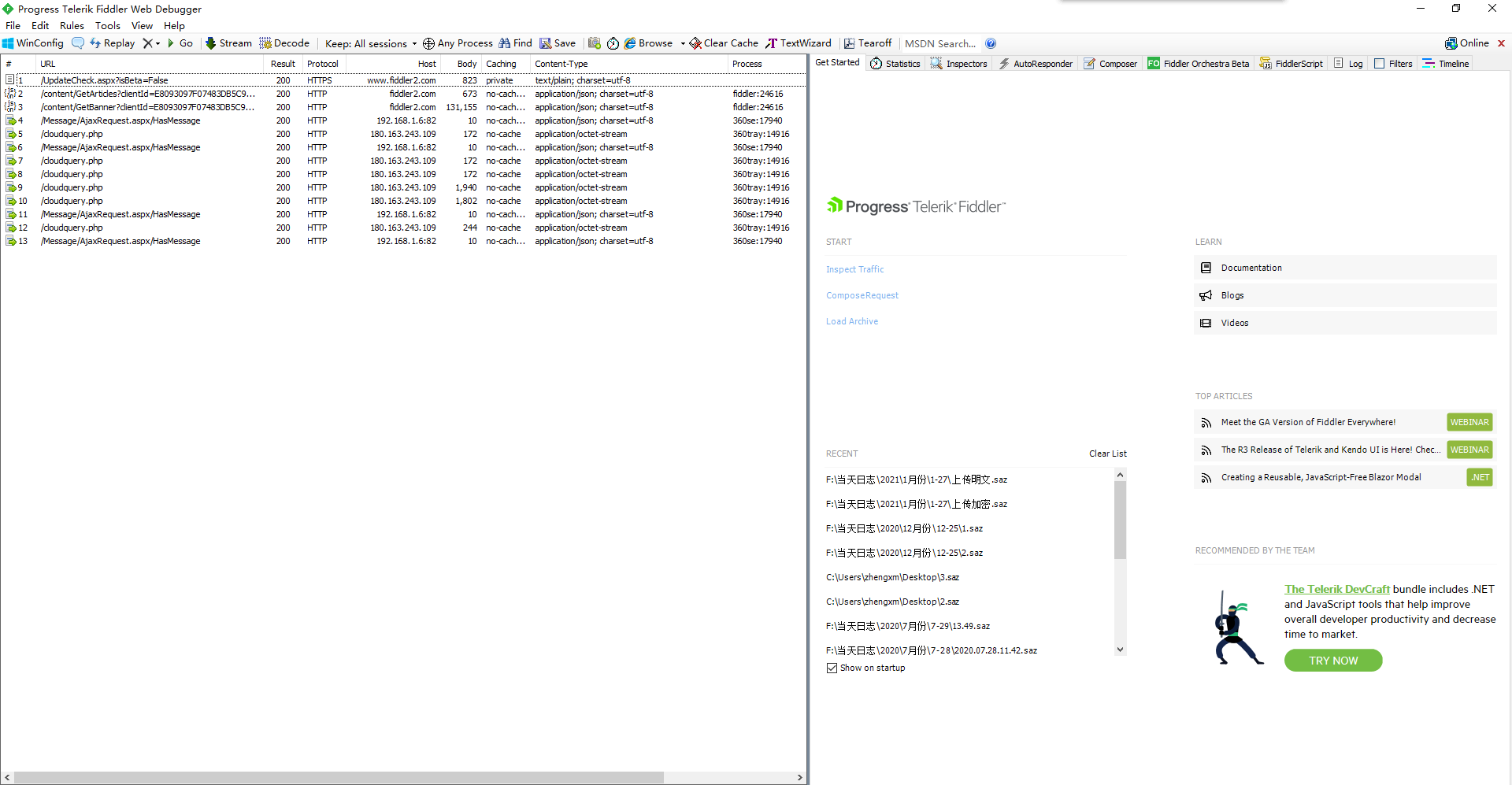
# 网络监听

## 2.1 Fiddler

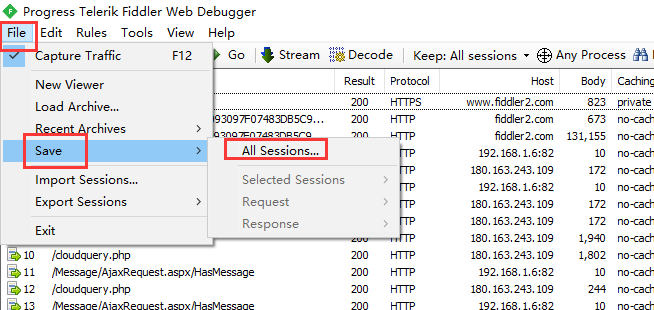
**Fiddler是一个http协议调试代理工具，它能够记录并检查所有你的电脑和互联网之间的http通讯，设置断点，查看所有的"进出"Fiddler的数据(指[cookie](https://baike.so.com/doc/3766187-3956334.html" \t "https://baike.so.com/doc/_blank),html,js,css等文件)。 Fiddler 要比其他的网络调试器要更加简单，因为它不仅仅暴露http通讯还提供了一个用户友好的格式。**

操作步骤及演示

操作步骤：将fiddle安装包放到客户终端电脑上进行安装，安装完成后，运行打开，打开界面，默认打开即监控，如下图所示。



重现问题后，需要即时保存监控数据成文件。该存储格式为.saz



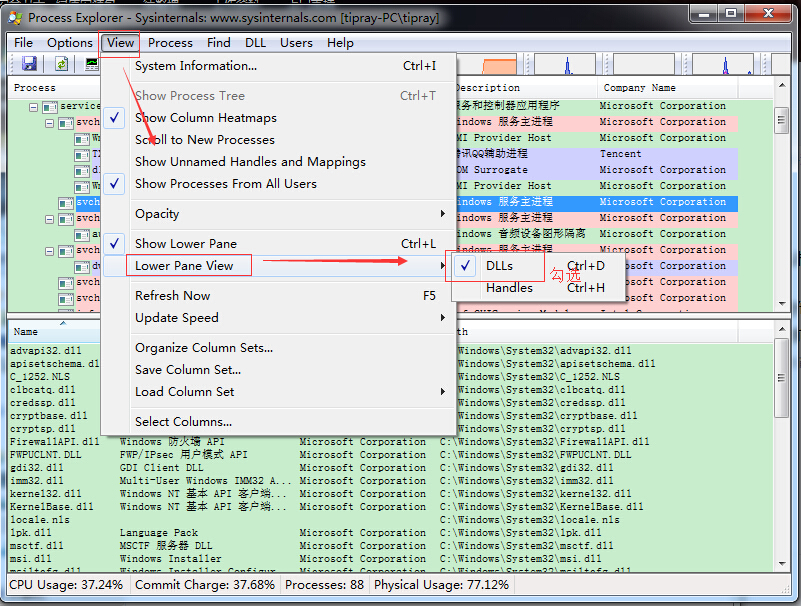
# 进程钩子

## 3.1 Procexp

### **Processxp工具是一款拥有功能强大的监视和过滤的高级Windows进程监视器工具，可查看进程加载组件**

* 操作步骤

步骤一：运行procexp.exe，打开后需要操作设置-view-LowerPaneView-DLLs，入下图所示



步骤二：点击打开加密文件的软件进程，wps.exe然后下面可以看到有。

# 系统工具

## 4.1(磁盘硬盘占用率分割工具)SpaceSniffer

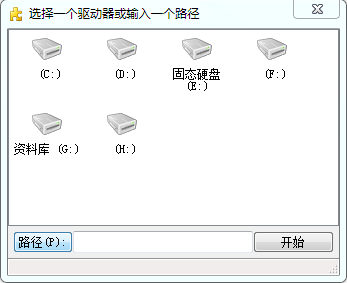
### **4.1.1SpaceSniffer是一个可以查看硬盘中文件和文件夹的分布情况的应用程序**

* 操作步骤及演示

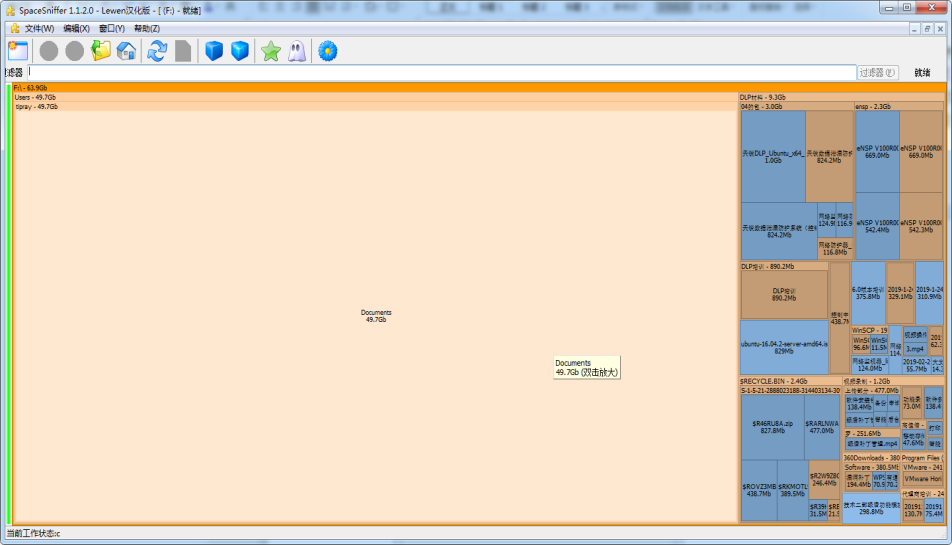
步骤一：找到对应的SpaceSniffer程序，双击运行打开。



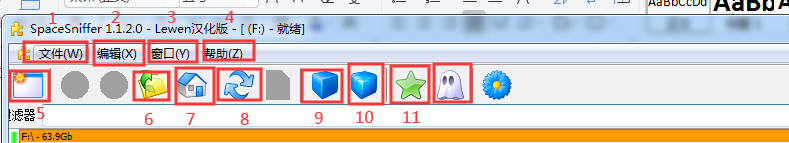
步骤二：运行SpaceSniffer时会弹出一个窗口，用来选择要分析的磁盘。如果不想分析整个分区，还可以点击“路径”按钮来分析某个文件夹。选择好需要分析的分区或文件夹后，点击“开始”开始分析就可以了。



步骤三：选中F盘符后，点击开始，会自动分析F盘中文件和文件夹的分布情况。SpaceSniffer分析的速度非常快，并且会以区块大小来表示文件占用硬盘的空间大小，橙色表示磁盘，褐色表示文件夹，蓝色表示文件(如图所示)。在文件夹的区块上双击就可以查看文件夹里面的文件分布，也可以用鼠标右键点击查看。同在文件夹当中的操作一样，用户可以直接选择删除文件或文件夹。



步骤四：了解软件菜单栏



1. 点击文件，可以选择新建或者导出。新建可选择次磁盘或者文件夹路径。导出可以导出当前磁盘分区的文件报告，可进行查看。
2. 编辑可选择配置。配置中包含（图形、效果、动作、颜色）
3. 图形可设置是否显示空闲空间、是否做项目排序、是否显示未知空间、字体大小调节、最小单元尺寸（像素）调节、比例调节、初始详情级别调节
4. 效果可设置是否动态缩放、缩放时间长短调节、刷新延迟时间调节
5. 动作可设置是否交替数据流扫描、是否扫描后闪动窗口、是否鼠标焦点改变时保持图像提示工具条、是否弹出事件日志控制台、是否勾选日志扫描警告
6. 颜色可设置驱动器颜色、可用空间颜色、文件夹颜色、未知空间颜色、文件颜色、鼠标悬停、鼠标离开、水平对比、边界对比、高亮显示
7. 窗口，可设置显示日志控制台、水平平铺、纵向平铺、层叠、全部最小化、关闭。主要是对窗口进行设置的
8. 帮助：过滤器帮助、标签帮助、命令行帮助、支持本程序、关于。该地方是对程序一些功能的帮助提示，可参考使用。
9. 该图标是选择需要分析的磁盘或者路径
10. 该图标是选择上一级
11. 该图标是显示起始目录
12. 该图标是新建一个扫描
13. 精简信息
14. 更多详细信息
15. 显示可用空间
16. 过滤器：可参考帮助-过滤器帮助，可设置过滤条件进行筛选

# 其他工具

## **5.1UltraEdit-32**

### **5.1.1主要用于查看加密文件编码和查看终端运行日志。可通过此软件判断文件是几代加密文件，文件编码是否有丢失**

UltraEdit-32是能够满足你一切编辑需要功能强大的文本编辑器，ultraedit可以编辑文本、十六进制、ASCII码，可以取代记事本，内建英文单字检查、C++及VB指令突显，可同时编辑多个文件，而且即使开启很大的文件速度也不会慢。UltraEdit-32软件附有HTML标签颜色显示、搜寻替换以及无限制的还原功能，一般大家喜欢用其来修改EXE或DLL文件。

在绿盾问题排查中，主要用于查看加密文件编码和查看终端运行日志。